ABSTRACT

A pseudorandom number generator (1) has a first linear feedback shift register (2), a second linear feedback shift register (3), an initial value generator (4), a polynomial coefficient generator (5), and a pseudorandom number output unit (6). The initial value generator (4) generates initial values and supplies the same to the first linear feedback shift register (2) and second linear feedback shift register (3). The polynomial coefficient generator (5) generates coefficients of a characteristic polynomial and supplies the same to the second linear feedback shift register (3). The pseudorandom number output unit (6) carries out exclusive-OR operations on bits sequentially provided by the first linear feedback shift register (2) and second linear feedback shift register (3), generates a pseudorandom number sequence, and outputs the same.